Università degli Studi di Milano

Laurea in Sicurezza dei sistemi e delle reti informatiche

Note di logica proposizionale

STEFANO FERRARI

Fondamenti di informatica per la sicurezza

Indice

1. Tavole di verità

La semantica dei connettivi è illustrata dalle seguenti tabelle, dette *tabelle di verità*:

a	b	$a \vee b$	$a \wedge b$	$\neg a$	$a \rightarrow b$	$a \leftrightarrow b$
F	F	F	F	V	V	V
F	V	V	F	V	V	F
V	F	V	F	F	F	F
V	V	V	V	F	V	V

2. Le dimostrazioni

Le dimostrazioni sono probabilmente l'ostacolo maggiore del corso di Fondamenti di informatica per la sicurezza.

Il motivo di tale osticità è che non esiste un metodo semplice per effettuarle.

In un ambito non complesso quale la teoria della logica proposizionale, qualsiasi teorema è dimostrabile per elencazione e verifica dei casi possibili. Tuttavia al crescere dei simboli enunciativi coinvolti, il numero di casi da verificare cresce esponenzialmente (dimostrazioni che coinvolgono N termini, richiedono, in generale, 2^N interpretazioni).

Poiché non è fattibile, in generale, una dimostrazione diretta, è utile (se non necessaria) una modalità dimostrativa che non richieda di analizzare tutte le possibili configurazioni dei termini in gioco. Tipicamente, la dimostrazione viene effettuata con una modalità costruttiva: a partire dalle assunzioni iniziali, si ottiene la tesi iterando l'applicazione di regole dimostrative.

Anche in questo caso, tuttavia, non esiste un procedimento che permetta di ottenere la dimostrazione con il minor numero di passi possibile (se non analizzando esaustivamente tutte le possibili sequenze di passi dimostrativi). Il procedimento utilizzato di solito è di tipo *trial-and-error* (prova e sbaglia) ed è basato su un po' di "fiuto" da affinare con l'esperienza.

2.1 Definizione

Un *teorema* della logica proposizionale è costituito da:

- una o più proposizioni , a_k $(1 \leq k \leq n)$, dette *assunzioni* o *ipotesi*;
- da una proposizione, t, detta *tesi*.

La congiunzione delle ipotesi deve implicare la tesi. Pertanto, un teorema è esprimibile come:

$$a_1 \wedge \cdots \wedge a_n \Rightarrow t$$

Una *dimostrazione* può essere formulata come una sequenza di proposizioni vere $p_1, \ldots, p_m$, dove p_j, $1 \leq j \leq m$:

- è un'assunzione;
- è una tautologia;
- è ottenuta per applicazione delle regole di inferenza;
- p_m è la tesi.

$$\{t_1, \ldots, t_k\} \cup \{a_1, \ldots, a_n\}$$
$$\downarrow$$
$$\{t_1, \ldots, t_k\} \cup \{a_1, \ldots, a_n\} \cup \{b_1, \ldots, b_m\}$$
$$\downarrow$$
$$\{t_1, \ldots, t_k\} \cup \{a_1, \ldots, a_n\} \cup \{b_1, \ldots, b_m\} \cup \{c_1, \ldots, c_h\}$$
$$\downarrow$$
$$\ldots$$
$$\downarrow$$
$$\{t_1, \ldots, t_k\} \cup \{a_1, \ldots, a_n\} \cup \{b_1, \ldots, b_m\} \cup \{c_1, \ldots, c_h\} \cup \cdots \cup \{z_1, \ldots, z_i = \boldsymbol{th}, \ldots, z_j\}$$

Figura 1: Una dimostrazione può essere vista come la deduzione della tesi a partire dall'insieme delle tautologie e delle ipotesi, mediante un ampliamento reiterato dell'insieme delle proposizioni vere.

Quindi una dimostrazione deve essere costituita solo da proposizioni la cui veridicità viene assicurata dall'essere una delle assunzioni (per ipotesi vere), una tautologia (cioè una proposizione sempre vera), o una proposizione ottenuta applicando una regola d'inferenza.

Le *regole di inferenza* sono regole che permettono di dedurre una proposizione valida a partire da un insieme di proposizioni (vere). Esse sono di quattro tipi:

- dato che p è vera e p equivale a q ($p \Leftrightarrow q$), anche q è vera (*equivalenza logica*);
- se p è una tautologia e a è una sua proposizione componente, sostituendo a tutte le occorrenze di a in p la proposizione q, si ottiene ancora una tautologia (*sostituzione*);
- dato che $p \rightarrow q$ e p sono entrambe vere, si deduce che anche q è vera (*modus ponens*);
- dato che $p \rightarrow q$ e $\neg q$ sono entrambe vere, si deduce che anche $\neg p$ è vera (*modus tollens*).

In sostanza, una regola di inferenza è un meccanismo che permette di ottenere una proposizione vera a partire da un insieme di proposizioni vere. Le regola di inferenza, quindi, permettono di ampliare l'insieme delle proposizioni che si sa essere vere.

Quindi, una dimostrazione può essere vista come un procedimento che, a partire dall'unione dell'insieme delle tautologie e dell'insieme delle ipotesi, aggiunge via via elementi all'insieme delle proposizioni vere, fino ad includere la tesi in questo insieme.

Come schematizzato in fig. 1, questo procedimento può essere formalizzato come segue. Dato l'insieme delle tautologie, $T = \{t_1, \ldots, t_k\}$, e l'insieme delle ipotesi, $A = \{a_1, \ldots, a_n\}$, l'insieme delle proposizioni vere all'inizio della dimostrazione è dato da $T \cup A$. L'applicazione delle regole di inferenza a $T \cup A$ consente di ottenere un insieme di nuove proposizioni vere, $B = \{b_1, \ldots, b_m\}$, che vanno ad aggiungersi alle precedenti, ottenendo così $T \cup A \cup B$. Iterando l'applicazione delle regole d'inferenza, si ottengono via via nuovi insiemi di proposizioni vere, fino ad ottenere un insieme, nell'esempio riportato in figura l'insieme $Z = \{z_1, \ldots, z_j\}$, il quale contiene la tesi, th.

Per semplicità, nella pratica, la dimostrazione si limita ad elencare le proposizioni strettamente necessarie per arrivare alla tesi. Vengono quindi introdotte le ipotesi solo se e quando servono e le tautologie che, eventualmente, risultano necessarie. Invece di elencare tutte le nuove proposizioni ottenibili dall'applicazione esaustiva delle regole d'inferenza all'insieme delle proposizioni vere dato, si esplicitano solo le proposizioni necessarie alla dimostrazione (accompagnate dalla regola d'inferenza che motiva la veridicità della proposizione).

2.2 Un primo esempio

Sia dato il seguente teorema:

Ip1 a

Ip2 $a \rightarrow b$

Tesi b

Il teorema sopra riportato è costituito da due ipotesi e fa uso di due termini (a e b).

Informalmente, l'ipotesi Ip2 dice che se a è vero, allora lo è anche b. Ma l'Ip1 dice che, in effetti, a è vero. Allora si può dedurre che anche b sia vero, dimostrando così la tesi.

Più formalmente, abbiamo un'implicazione (Ip2) di cui sappiamo che la premessa è vera (Ip1). Possiamo quindi applicare la regola di inferenza detta *modus ponens*, che ci permette di inferire la veridicità della conseguenza dell'implicazione considerata.

Il ragionamento di cui sopra lo si può formalizzare come:

(1)	a	Ip1
(2)	$a \rightarrow b$	Ip2
(3)	b	Modus Ponens da (1) e (2)

Ogni riga della dimostrazione contiene un numero incrementale che identifica il passo (e.g., (3)), la proposizione introdotta (e.g., b) e la motivazione (e.g., Modus Ponens da (1) e (2)). Se la motivazione è una regola di inferenza, deve riportare le proposizioni a cui viene applicata. Se invece è una tautologia, deve essere riportato il nome della tautologia.

2.3 Le regole d'inferenza

Modus ponens e modus tollens

Nel paragrafo 2.2, è stata introdotto l'uso del modus ponens. Modus ponens e modus tollens sono le regole di inferenza più utilizzate (o, meglio, utilizzate in modo esplicito) per produrre nuove proposizioni e vanno capite bene.

Entrambe si basano su una implicazione. Il modus ponens permette di dedurre la veridicità della conseguenza data la veridicità della premessa. Il modus tollens, invece, permette di dedurre la falsità della premessa data la falsità della conseguenza.

La correttezza di queste regole può essere compresa analizzando la tavola di verità dell'implicazione:

a	b	$a \rightarrow b$
F	F	V
F	V	V
V	F	F
V	V	V

In entrambe le regole, si ha che l'implicazione $a \rightarrow b$ è vera. Quindi la riga in cui l'implicazione è falsa può essere cancellata:

a	b	$a \rightarrow b$
F	F	V
F	V	V
~~V~~	~~F~~	~~F~~
V	V	V

Nel caso del modus ponens, si ha che la premessa, a, è vera, perciò, cancellando le prime due righe della tabella, che non rispettano questa condizione, si ha:

a	b	$a \rightarrow b$
~~F~~	~~F~~	~~V~~
~~F~~	~~V~~	~~V~~
~~V~~	~~F~~	~~F~~
V	V	V

da cui risulta chiaro che anche la conseguenza, b, deve essere vera.

Nel caso del modus tollens, si ha che la conseguenza, b, è falsa, perciò, cancellando le due righe della tabella, che non rispettano questa condizione, si ha:

a	b	$a \rightarrow b$
F	F	V
~~F~~	~~V~~	~~V~~
~~V~~	~~F~~	~~F~~
~~V~~	~~V~~	~~V~~

da cui risulta chiaro che anche la premessa, a, deve essere falsa.

Equivalenza logica

L'uso della equivalenza logica come regola d'inferenza è abbastanza intuitivo. Si tratta di introdurre una proposizione in quanto equivalente (non per forma, ma per valori di verità) ad una proposizione già dimostrata vera (e quindi citata nei passi di dimostrazione precedenti). Pertanto, anche la nuova proposizione sarà vera (esattamente come la proposizione ad essa equivalente).

Sostituzione

La sostituzione, infine, permette di adattare una tautologia al caso dato dal teorema in esame. Per ogni tautologia, infatti, per qualsiasi interpretazione dei termini che la compongono, il valore di verità corrispondente è sempre V. Pertanto, ad ogni termine di una tautologia possiamo sostituire una qualsiasi proposizione (purché tale sostituzione avvenga per tutte le occorrenze di tale termine) e la proposizione risultante resterà sempre una tautologia. Per esempio, alla tautologia $a \vee \neg a$ possiamo applicare la sostituzione $a \rightsquigarrow (b \wedge c)$, ottenendo $(b \wedge c) \vee \neg(b \wedge c)$, che risulterà essere ancora una tautologia.

La sostituzione viene applicata, generalmente, in modo implicito (per non appesantire la dimostrazione).

2.4 Esempio d'uso di modus tollens

Sia dato il teorema:

Ip1 $b \rightarrow \neg a$

Ip2 a

Tesi $\neg b$

Intuitivamente (ma se c'è di mezzo un'implicazione non bisogna mai fidarsi troppo di una spiegazione intuitiva), si può ragionare così: se b fosse vera, a sarebbe falsa; poiché a è vera, b non può essere vera (perché a dovrebbe essere falsa), perciò b deve essere falsa.

Formalmente:

(1)	$b \rightarrow \neg a$	Ip1
(2)	a	Ip2
(3)	$\neg b$	M. Tollens da (1) e (2)

Da notare che, poiché una dimostrazione è una sequenza di proposizioni vere, la proposizione "b è falsa" va scritta "è vera la negazione di b", cioé $\neg b$.

2.5 Tautologie

Le tautologie usate nelle dimostrazioni sono spesso implicazioni logiche o equivalenze logiche. La loro naturà è differente, così come il loro uso nelle dimostrazioni.

Una equivalenza logica è una relazione che lega due proposizioni che assumono gli stessi valori logici per qualsiasi interpretazione dei loro termini. Essa lega quindi due proposizioni tra di loro interscambiabili. Pertanto, una equivalenza logica permette di modificare una qualsiasi proposizione che contenga una delle due proposizioni logicamente equivalenti, sostituendo ad tale proposizione quella ad essa equivalente.

Per esempio, la legge di De Morgan dice che proposizione $\neg(a \wedge b)$ equivale alla proposizione $\neg a \vee \neg b$. Quindi, la proposizione $(\neg c \wedge (\neg a \vee \neg b)) \rightarrow (c \vee a)$ sarà equivalente alla proposizione $(\neg c \wedge \neg(a \wedge b)) \rightarrow (c \vee a)$, per tutte le interpretazioni di a, b, c. La proposizione equivalente è stata ottenuta sostituendo $\neg a \vee \neg b$ con $\neg(a \wedge b)$ nella proposizione di partenza.

Una implicazione logica, invece, non consente la sostituzione di parti di una proposizione. Le implicazioni logiche sono utili per poter applicare il modus ponens o il modus tollens. Esse consentono, cioé, di affermare la validità di una proposizione.

Per esempio, l'eliminazione della congiunzione $(a \wedge b \Rightarrow a)$ consente di semplificare una proposizione quando essa sia costituita da uno o più congiunzioni. Data la validità della proposizione $(a \rightarrow b) \wedge (c \rightarrow a)$, è possibile affermare la validità di $(a \rightarrow b)$. Volendo essere più formali, tale inferenza dovrebbe passare per l'applicazione del modus ponens, come segue:

(1)	$(a \rightarrow b) \wedge (c \rightarrow a)$	Ipotesi
(2)	$((a \rightarrow b) \wedge (c \rightarrow a)) \rightarrow (a \rightarrow b)$	Eliminazione di congiunzione
(3)	$(a \rightarrow b)$	Modus Ponens da (1) e (2)

Per rendere più leggera la dimostrazione, tuttavia, è accettabile semplificarla nel seguente modo:

(1)	$(a \rightarrow b) \wedge (c \rightarrow a)$	Ipotesi
(2)	$(a \rightarrow b)$	Elim. di congiunzione (1)

Le informazioni per comprendere le motivazioni adotte ci sono tutte, ma si evita un passaggio (scontato) per il modus ponens.

Utilizzare una inferenza logica come se fosse una equivalenza logica porta spesso a risultati sbagliati. Per esempio, l'applicazione della eliminazione di congiunzione per semplificare una proposizione è uno degli errori più comuni. Ottenere $\neg a$ applicando l'eliminazione della congiunzione a $\neg(a \wedge b)$ è sbagliato, come un breve ragionamento rende evidente: se a fosse vero e b fosse falso, $\neg(a \wedge b)$ sarebbe vero, ma $\neg a$, che si otterrebbe applicando l'eliminazione di congiunzione come se fosse una tautologia, sarebbe falso.

Di seguito, si analizzano alcune tautologie che ricorrono spesso nelle dimostrazioni.

Eliminazione di congiunzione

L'eliminazione di congiunzione:

$$a \wedge b \Rightarrow a$$

può essere compresa osservando la tavola di verità della congiunzione, dove risulta evidente che la congiunzione può essere vera solo se sono vere entrambe le proposizioni componenti.

Ne risulta che, se la congiunzione di due proposizioni è vera, lo devono essere anche le singole componenti.

Pertanto, per esempio, dalla proposizione $p \wedge (q \vee r)$ può essere dedotto tanto p quanto $q \vee r$.

Un uso errato dell'eliminazione della congiunzione consiste nell'applicarla come se fosse una semplificazione. Per esempio, è sbagliato usare $(b \wedge c) \rightarrow a$ per dedurre $b \rightarrow a$, motivandolo con l'eliminazione della congiunzione.

Introduzione di disgiunzione

L'introduzione di disgiunzione:

$$a \Rightarrow a \vee b$$

può essere compresa osservando la tavola di verità della disgiunzione, dove risulta evidente che affinché la disgiunzione sia vera è sufficiente che lo sia una sola delle proposizioni componenti.

Pertanto, disgiungendo una proposizione vera con una qualsiasi proposizione, la proposizione composta così ottenuta è vera.

Per esempio, dalla proposizione $p \wedge q$ si può dedurre $(p \wedge q) \vee \neg r$.

Un uso errato dell'introduzione della disgiunzione consiste nell'applicarla come se fosse una espansione. Per esempio, è sbagliato usare $b \rightarrow a$ per dedurre $(b \wedge c) \rightarrow a$, motivandolo con l'introduzione della disgiunzione.

Definizione di implicazione

La definizione di implicazione:

$$a \rightarrow b \Leftrightarrow \neg a \vee b$$

è una proposizione vera, appunto, per definizione del connettivo $\rightarrow$.

Questa tautologia è utile per trasformare una disgiunzione in una implicazione (che poi può essere usata per una inferenza tramite modus ponens/tollens) o, al contrario, per trasformare una implicazione in una più maneggevole disgiunzione.

Per esempio, dalla proposizione $(a \vee b) \rightarrow c$ si può dedurre $\neg(a \vee b) \vee c$. Ciò consente di dedurre $(\neg a \wedge \neg b) \vee c$, per le leggi di De Morgan e poi $(\neg a \vee c) \wedge (\neg b \vee c)$ per la distributività. Da quest'ultima proposizione, mediante l'applicazione della eliminazione di congiunzione, si possono ottenere sia $\neg a \vee c$ sia $\neg b \vee c$, che sono proposizioni più semplici di quella iniziale.

Sempre applicando la definizione di implicazione alle proposizioni così ottenute si può dedurre $a \rightarrow c$ oppure $b \rightarrow c$.

Definizione di biimplicazione

La definizione di biimplicazione è disponibile in due forme, tra di esse logicamente equivalenti:

$$a \leftrightarrow b \Leftrightarrow (a \rightarrow b) \wedge (b \rightarrow a)$$

e

$$a \leftrightarrow b \Leftrightarrow (a \wedge b) \vee (\neg a \wedge \neg b)$$

Può essere usata per semplificare una proposizione complessa, o, al contrario, per dimostrare l'equivalenza di due proposizioni.

Per esempio, la proposizione $(a \vee b) \leftrightarrow c$ può essere usata per dedurre $((a \vee b) \rightarrow c) \wedge (c \rightarrow (a \vee b))$. Da questa, per esempio, può risultare utile dedurre $c \rightarrow (a \vee b)$ che può essere usato per ottenere la forma equivalente $\neg c \vee (a \vee b)$, dalla quale si ottiene $(\neg c \vee a) \vee b$ (per associatività), la quale a sua volta può essere usata per ottenere una formula implicativa $\neg(\neg c \vee a) \rightarrow b$ o la sua equivalente $(c \wedge \neg a) \rightarrow b$ (per le leggi di De Morgan). Va sottolineato che l'ultimo passo ha inglobato una doppia negazione (è stato usato c anziché $\neg\neg c$).

Volendo invece dimostrare la biimplicazione di due proposizioni, si può dimostrare che una implica l'altra e che l'altra implica l'una.

Dimostrazione per casi

La dimostrazione per casi consiste nel suddividere l'insieme delle situazioni possibili in più sottoinsiemi e poi dimostrare la tesi per ogni singolo sottoinsieme. In sostanza, si predispone una opportuna casistica che vada a coprire tutti i casi possibili, e poi si dimostra che la tesi è valida in ogni caso. È un po' come se uno dicesse: "Se piove, vado al cinema, e, se non piove, vado al cinema lo stesso.". Non è che il Tizio in questione andrà forse al cinema?

In logica proposizionale si possono avere solo due casi: vero o falso. Pertanto, la dimostrazione per casi si limita a dimostrare che la tesi è logicamente implicata sia nel caso in cui una data proposizione è vera sia quando questa proposizione è falsa.

Formalmente, questa tecnica dimostrativa può essere espressa come:

$$(a \rightarrow b) \wedge (\neg a \rightarrow b) \Rightarrow b$$

Il fatto che b sia implicato contemporaneamente sia da una proposizione a sia dalla sua negazione, $\neg a$, significa che b è vero indipendentemente dal valore assunto da a.

In una dimostraizone, per poter applicare la dimostrazione per casi è necessario che prima sia dimostrata la validità di $a \rightarrow b$ e la validità di $\neg a \rightarrow b$. Da ciò deriva la validità di $(a \rightarrow b) \wedge (\neg a \rightarrow b)$. Poiché, $(a \rightarrow b) \wedge (\neg a \rightarrow b) \rightarrow b$ è vera (è una tautologia!), si ha che è vera sia una implicazione, sia la premessa dell'implicazione. È quindi applicabile il modus ponens per ottenere la validità della conseguenza, in questo caso, b.

Per esempio, il seguente teorema

Ip1 $\neg a \rightarrow (b \vee c)$

Ip2 $\neg(b \vee c) \vee a$

Tesi a

può essere dimostrato per casi:

(1)	$\neg a \rightarrow (b \vee c)$	Ip1
(2)	$\neg(b \vee c) \rightarrow a$	Contrapposizione (1)
(3)	$\neg(b \vee c) \vee a$	Ip2
(4)	$(b \vee c) \rightarrow a$	Def. implicazione (3)
(5)	$((b \vee c) \rightarrow a) \wedge (\neg(b \vee c) \rightarrow a)$	Congiunzione di (4) e (2)
(6)	$(((b \vee c) \rightarrow a) \wedge (\neg(b \vee c) \rightarrow a)) \rightarrow a$	Dimostrazione per casi
(7)	a	M. Ponens da (5) e (6)

Nell'esempio, si dimostra che a è vero indipendentemente dal valore di verità assunto da $b \vee c$. Ciò permette di concludere che a deve essere vero.

Dimostrazione per assurdo

La dimostrazione per assurdo è una tecnica dimostrativa che consiste nell'utilizzare un'ipotesi aggiuntiva per giungere ad una contraddizione. Questo consente di concludere che l'ipotesi aggiuntiva è falsa. Se l'ipotesi aggiuntiva consiste nella negazione della tesi, il percorso dimostrativo si conclude nella dimostrazione della tesi stessa.

La dimostrazione per assurdo, che in logica proposizionale si riduce ad una riformulazione del modus tollens, può essere formalizzata dalla seguente tautologia:

$$(\neg b \rightarrow a) \wedge \neg a \Rightarrow b$$

2.6 Verifica di correttezza di dimostrazioni

Come si capisce se una dimostrazione è corretta?

Dati i passaggi dimostrativi e le motivazioni, una verifica di correttezza è abbastanza semplice.

Tuttavia, soprattutto quando non si è sicuri dell'uso degli strumenti dimostrativi, sarebbe utile disporre di un algoritmo alternativo per la verifica della correttezza delle dimostrazioni. Tale algoritmo, una specie di prova del nove che dovrebbe essere basato solo sulla correttezza sintattica, non esiste.

Però, la definizione di dimostrazione data nel paragrafo 2.1 permette di stabilire alcune condizioni che permettono di valutare se la dimostrazione è sbagliata. Ciò, nella maggior parte dei casi, è abbastanza per consentire l'autovalutazione delle proprie dimostrazioni.

Per definizione, date un insieme di n proposizioni, dette ipotesi, $\{a_i \,|\, i = 1, \ldots, n\}$, e una proposizione t, detta tesi, la proposizione:

$$a_1 \wedge \cdots \wedge a_n \rightarrow t$$

deve essere una tautologia.

Per esempio, nel caso una dimostrazione risultasse particolarmente ostica, la stesura della tavola di verità della proposizione precedente può eliminare il dubbio della presenza di un errore di stampa che infici la validità del teorema.

La dimostrazione avviene per passi dimostrativi, ognuno dei quali specifica una asserzione, p_i. Tale proposizione deve essere una derivazione logica delle ipotesi e delle asserzioni precedenti, $\{p_k \,|\, k = 1, \ldots, i-1\}$. Per ogni passo, i, cioè, la seguente proposizione:

$$a_1 \wedge \cdots \wedge a_n \wedge p_1 \wedge \cdots \wedge p_{i-1} \rightarrow p_i$$

deve essere una tautologia.

Poiché molti passi dimostrativi condividono molte sottoproposizioni, la stesura della tabella di verità di ogni passo non risulta troppo dispendiosa, e, oltre ad essere un utile esercizio, può conferire una certa confidenza nell'effettuazione delle dimostrazioni.

2.7 Esempi di dimostrazione di teoremi

Esempio 1

Dimostrare il seguente teorema:

Ip1 $(c \wedge b) \vee a$

Ip2 $\neg b$

Tesi a

Dimostrazione:

(1)	$(c \wedge b) \vee a$	Ip1
(2)	$(c \vee a) \wedge (b \vee a)$	equiv. logica a (1)
(3)	$b \vee a$	Elim. di cong. (2)
(4)	$\neg b \rightarrow a$	equiv. logica a (3)
(5)	$\neg b$	Ip2
(6)	a	M. Ponens da (4) e (5)

È possibile anche un'altra soluzione. Informalmente:

- b è falso (Ip2)
- se b è falso, anche $(c \wedge b)$ è falso
- poiché $(c \wedge b) \vee a$ è vero (Ip1), a deve essere vero
- quindi la tesi è dimostrata

Più formalmente:

- $\neg b$ è vero (Ip2)
- $\neg b \rightarrow (\neg b \vee \neg c)$ (Aggiunta di disgiunzione)
- $\neg b \vee \neg c$ (modus ponens tra le precedenti affermazioni)
- $\neg(b \wedge c)$ (Leggi di De Morgan)
- $\neg(c \wedge b) \rightarrow a$ (equiv. logica a Ip1)
- a (modus ponens tra le precedenti proposizioni)

E quindi:

(1)	$\neg b$	Ip2
(2)	$\neg b \rightarrow (\neg b \vee \neg c)$	Aggiunta di disgiunzione
(3)	$\neg b \vee \neg c$	M. Ponens da (1) e (2)
(4)	$\neg(b \wedge c)$	Leggi di De Morgan a (3)
(5)	$(c \wedge b) \vee a$	Ip1
(6)	$\neg(c \wedge b) \rightarrow a$	equiv. logica a (5)
(7)	a	M. Ponens da (4) e (6)

Da notare che i passi (2) e (3) sono forse eccessivamente formali. Al passo (2) è stata introdotta una tautologia ed è stata usata come implicazione per poi applicare un modus ponens. Sebbene formalmente corretto, il passo (2) poteva essere evitato, perdendo in formalità, ma guadagnando in leggibilità. In tal caso, il passo (3) sarebbe stato motivato con "Aggiunta di disgiunzione a (1)".

Esempio 2

Dimostrare il seguente teorema:

Ip1 $\neg a \rightarrow (b \vee c)$

Ip2 $\neg a \wedge \neg b$

Tesi c

Dimostrazione:

(1)	$\neg a \wedge \neg b$	Ip2
(2)	$\neg a$	Eliminazione di congiunzione da (1)
(3)	$\neg a \rightarrow (b \vee c)$	Ip1
(4)	$b \vee c$	M. Ponens da (2) e (3)
(5)	$\neg b \rightarrow c$	Definizione di implicazione (4)
(6)	$\neg b$	Eliminazione di congiunzione da (1)
(7)	c	M. Ponens da (5) e (6)

Il ragionamento seguito per individuare il percorso dimostrativo è basato sull'osservazione che la tesi è costituita da un unico termine (c) e che tale termine si trova solo nella prima ipotesi. Poiché la prima ipotesi è una implicazione, un buon tentativo può esser fatto con un modus ponens o un modus tollens. Poiché il termine c si trova nella conseguenza della prima ipotesi ($b \vee c$), il miglior candidato è il modus ponens.

Il modus ponens richiede che la premessa sia vera. Nel caso in esame, la premessa è $\neg a$. Un passo intermedio può quindi essere di cercare di dimostrare che $\neg a$ è vero.

Osservando la seconda ipotesi, questo risulta semplice. Quindi, è possibile dimostrare che la conseguenza della prima ipotesi, $b \vee c$ è vera.

L'applicazione della definizione di implicazione rende chiaro il rimanente passo: ottenendo $\neg b \rightarrow c$, basta dimostrare $\neg b$ per pervenire alla tesi. Cosa che può essere fatta osservando che la seconda ipotesi fornisce proprio questa proposizione.

Esempio 3

Dimostrare il seguente teorema:

Ip1 $a \vee b \vee c$

Ip2 $(a \vee b) \rightarrow c$

Tesi c

Dimostrazione:

(1)	$a \vee b \vee c$	Ip1
(2)	$\neg(a \vee b) \rightarrow c$	Definizione di implicazione (1)
(3)	$(a \vee b) \rightarrow c$	Ip2
(4)	$(\neg(a \vee b) \rightarrow c) \wedge ((a \vee b) \rightarrow c)$	congiunzione di (2) e (3)
(5)	$((\neg(a \vee b) \rightarrow c) \wedge ((a \vee b) \rightarrow c)) \rightarrow c$	Dimostrazione per casi
(6)	c	M. Ponens da (4) e (5)

La dimostrazione è abbastanza semplice. È solo la complessità delle formule coinvolte che crea un po' di difficoltà di lettura.

Informalmente, la seconda ipotesi dice che c, la tesi, può essere dedotta da una data proposizione $(a \vee b)$. La prima ipotesi, opportunamente enunciata in una forma equivalente, dice che c può essere dedotta dalla negazione della premessa della seconda ipotesi, $\neg(a \vee b)$. Quindi, si può dire che c è vera indipendentemente dalla veridicità di $a \vee b$.

Questa conclusione è proprio la dimostrazione per casi: la tesi è vera per ogni possibile valore di $a \vee b$.

Esempio 4

Dimostrare il seguente teorema:

Ip1 a

Ip2 $(\neg a \wedge c) \vee \neg b$

Tesi $\neg b$

Dimostrazione:

(1)	$(\neg a \wedge c) \vee \neg b$	Ip2
(2)	$\neg(\neg a \wedge c) \rightarrow \neg b$	Definizione di implicazione (1)
(3)	$b \rightarrow (\neg a \wedge c)$	Contrapposizione (2)
(4)	$(b \rightarrow \neg a) \wedge (b \rightarrow c)$	Distributività delle conseguenze (3)
(5)	$b \rightarrow \neg a$	Elim. di congiunzione (4)
(6)	a	Ip1
(7)	$\neg b$	Modus Tollens da (5) e (6)

È possibile anche una dimostrazione alternativa:

(1)	$(\neg a \wedge c) \vee \neg b$	Ip2
(2)	$\neg(\neg a \wedge c) \rightarrow \neg b$	Definizione di implicazione (1)
(3)	$(a \vee \neg c) \rightarrow \neg b$	Leggi di De Morgan (2)
(4)	a	Ip1
(5)	$a \vee \neg c$	Introd. di disgiunzione (4)
(6)	$\neg b$	Modus Ponens da (3) e (5)

In quest'ultima dimostrazione al passo (3) si utilizza la legge di De Morgan per semplificare l'asserzione (2). La logica dimostrativa consiste nell'ottenere una implicazione e poi costruirne la premessa. Di questa dimostrazione è possibile una variante, dove la legge di De Morgan viene usata nella costruzione della premessa, anziché nella semplificazione dell'implicazione:

(1)	$(\neg a \wedge c) \vee \neg b$	Ip2
(2)	$\neg(\neg a \wedge c) \rightarrow \neg b$	Definizione di implicazione (1)
(3)	a	Ip1
(4)	$a \vee \neg c$	Introd. di disgiunzione (3)
(5)	$\neg\neg(a \vee \neg c)$	Doppia negazione (4)
(6)	$\neg(\neg a \wedge c)$	Leggi di De Morgan (5)
(7)	$\neg b$	Modus Ponens da (2) e (6)